ISSN. 1363-6650

JANUARY 1998
Issue 13

International Journal of FORENSIC COMPUTING™

Contents

International Journal of Forensic Computing

Third Floor, Colonnade House,
High Street, Worthing,
West Sussex, UK
BN11 1NZ

Tel: +44 (0) 1903 209226
Fax: +44 (0) 1903 233545
e-mail:ijfc@pavilion.co.uk
http:www.forensic-computing.com

Comment

Computer crime has suddenly become very big news. Those at the sharp end of investigation and prosecution have for years been warning about the power and potential of high-tech offences, as well as the problems in detecting and dealing with them.

For a long time politicians and senior law-enforcement figures across the world paid lip service to the situation but failed to take it seriously and were not prepared to invest fully in the necessary tools, techniques and staff to combat this relatively new field of crime.

However, a sea change is taking place, and everyone working in the industry will feel the repercussions.

Last month the Journal reported from the Internet conference in the US, which drew together some of the most important names and organisations dealing with the Net.

This month we feature the recent International Summit on computer crime and report on the discussions and findings by eight of the world's most powerful and richest countries.

One of the most important aspects of the international meeting is that countries are finally learning to pool their knowledge and resources so their respective law enforcement groups can work with each other.

Computer crime is global, and cyber criminals are known to use the tools of their illegal trade to communicate with each other. Indeed, contrary to the popular image of solitary "geek" hackers, most of them operate within cyber circles where information, tips and software are freely swapped.

It makes sense for police forces and investigators to team up in a similar way. Not only are new ideas propagated, but also the senselessness of duplicating work is avoided.

While this has been the case between some agencies in some countries for quite a while, the International Summit has ratified the process to make it the norm rather than the exception.

And by fully co-operating, a comprehensive approach can be taken towards the highly important issue of evidence recovery and forensic computing. At the moment just about every law enforcement group in every country has a different set of standards and methodology. It has been a case of suck it and see, which has resulted in several embarrassing and unnecessary legal defeats.

If police in one country are investigating a crime that could be prosecuted in another, it is vital they follow a set of agreed standards that leave no margin for error. Protocols like this will not happen overnight, but at least the ball is now rolling.

All eight countries have agreed on a set of principles and on an action plan to put them into effect. The points are fairly obvious (see page 14), but they are logical and leave little room for misinterpretation. The question now must be, to what extent will they be implemented? To tackle computer crime effectively, resources have to be quickly channelled into the appropriate areas; otherwise the summit's rhetoric will be meaningless.

By the next international gathering on computer crime, due to take place in May this year, it should be fairly obvious just how seriously the points have been put into action.

But if all goes to plan, and there is no reason why it shouldn't, the message to cyber criminals is stark: watch out – your life is about to get much harder.

together, we can ensure this dynamic new medium continues to grow and flourish, while protecting the copyright interests of hundreds of software companies."

"Now we are extending an invitation to server operators asking for their specific comments and suggestions on what could be appropriate next steps for SPA to take.

Those interested in finding out more can e-mail SPA at education@spa.org

AOL in battle with junk e-mailers

Internet service provider America Online has stopped a junk e-mailer that advertised pornographic Web sites from sending messages to its members.

Over the Air Equipment Inc surrendered in its fight against AOL and agreed to an injunction barring it from sending unsolicited e-mail to AOL subscribers.

AOL chairman and CEO Steve Case said: "Spammers have little regard for the people who receive their solicitations - a problem that's only magnified when a child is on the receiving end of an objectionable piece of junk e-mail.

"That's why we're going to continue to use every tool at our disposal to fight against spam and work toward a long-term solution to this problem, which affects all Internet users."

Over the Air Equipment, which until recently was sending AOL members hundreds of thousands of junk e-mails a day advertising its pornographic Web sites, agreed to a court order which stops the company from ever sending unsolicited e-mail to AOL members again.

And the firm also agreed to pay AOL a substantial, but undisclosed, sum of money in damages.

The AOL suit, which was filed Oct. 2, 1997, accused Over the Air Equipment of using deceptive practices, including falsifying e-mail transmission data, to avoid AOL's mail controls and to repeatedly transmit vast quantities of unsolicited e-mail to AOL members.

When the preliminary injunction was issued, the judge found that AOL's efforts to block junk e-mail were in the public interest and that it was likely to succeed on its claims of trespass and violations of the Computer Fraud and Abuse Act against Over the Air Equipment.

● AOL has announced that it has filed another suit against a junk e-mailer alleging that Squeaky Clean Marketing and Cyber Services, both based in Dallas, have ignored repeated requests to stop sending junk e-mail to members.

The complaint says that the two firms have sent millions of unsolicited e-mails selling everything from baldness cures to get-rich-quick schemes and that thousands of AOL member have complained.

AOL's suit alleges that both Squeaky Clean Marketing and Cyber Services are employing deceptive mailing practices to evade junk mail filters, including falsifying e-mail headers and relaying e-mails through third party computer networks to further camouflage the true source of the e-mails.

Staff rapped over Net porn

Two employees in Connecticut, US, were suspended and had their salaries cut for using state computers to access pornographic images on the Internet.

Both were suspended for three weeks without pay after the offences were discovered and officials say this was the first time state workers had been caught accessing Internet pornography.

In the case of Christopher Senecal, 29, a press secretary for the House Democrats, other employees complained about a slowdown in the legislative computer system.

An investigation revealed that Senecal had downloaded pornographic video on at least three occasions on his officially assigned computer.

He was then stripped of a recent promotion to senior press secretary, and his annual salary was slashed to $33,614 from $38,000.

The actions of George Mokritski, 45, were discovered after a supervisor reviewed a log of Internet activity by all legislative employees and Mokritski, administrative services coordinator for the joint committee on legislative management, had his salary cut to $40,845 from $43,000.

Web fights killer's parole

New York State Attorney General Dennis Vacco is urging people to speak out through the Internet to defeat a jailed child killer's bid for parole.

Vacco opposes parole for Joel Steinberg, who was found guilty of murdering six-year-old Lisa Steinberg a decade ago. The girl was brutally beaten and lay in a coma before she died.

Steinberg, an illegally practicing attorney, considered himself the girl's adoptive father and the case drew attention to the problem of child abuse in the US and sparked major law reforms.

Vacco said in a statement that New Yorkers could share their views about Steinberg's parole bid by contacting him on a new Web site accessible through the attorney general's home page.

He said: "Joel Steinberg should be forced to serve the maximum term of his sentence confined in a correctional facility of the state of New York. He has not yet paid his debt to society."

UK copyright, designs and patents law

The Copyright and Rights in Databases Regulations 1997, came to force in the UK this month.

The regulations, which implement the European Commission Database Directive on the legal protection of databases, are claimed to protect the investment of money, time, and effort that goes into compiling databases.

Announcing the new legislation, Ian McCartney, the Department of Trade's Minister of State in the UK said: "It will also give an important boost to the wider development of the information society."

According to the DTI, the regulations make certain changes to the system of copyright for databases. The regulations create an important new, free-standing, right to be known as "database right."

This is a right to prevent the unauthorised extraction of the whole or a substantial part of the contents of a database.

McCartney says the Regulations maintain the approach of copyright law and current exceptions will continue.

These, the DTI claims, relate for example to research, education, and libraries. The regulations also apply to database rights, the exceptions permitted by the new legislation, of which the most important are claimed to be those for illustration for non-commercial teaching and research.

Government spy computer snatched

A top secret data scrambling system used by the British Prime Minister went missing from Government offices.

The customised encryption computer was taken from the Cabinet Office next door to 10 Downing Street, the official Prime Minister's residence, in London.

According to government officials, the "spy computer system" was used for sending highly encrypted messages to the Prime Minister, Tony Blair, and the MI5/MI6 security services.

The computer, the size of a VCR, operates over wireline and wireless communications links.

However, who took the system is a mystery as the Cabinet Office is normally surrounded by police and even access to Downing Street itself is controlled by uniformed officers.

According to Scotland Yard, police are "investigating an allegation of theft from a government building in central London."

No other details about the theft, including the date of when the unit disappeared, have been released.

Although the Cabinet Office claims that there are no security problems associated with the apparent theft of the unit, the computer almost certainly uses the top secret Rambutan encryption system, which is claimed to be hacker-proof.

The Rambutan encryption system is normally chip-based and has a highly complex encryption algorithm developed by Cheltenham-based CESG, part of the Zergo group, to protect files and data communications.

It operates at speeds of up to 64,000 bits per second and is suitable for analogue modem communication, as well as analogue and digital radio links.

Swedish police swoop on alleged hackers

The computer systems of two Swedish teenagers have been confiscated by police after a year-long investigation.

No charges against the pair, who were both juveniles when the alleged offences took place, are said to have been brought, however.

The pair, now aged 15 and 18, were tracked down after they broke into the US Space Agency's computer system.

But the final straw for the Swedish authorities appears to be when they broke into the Web site of a Swedish county government agency and turned the page into a Web advert for pornography and marijuana.

Surprisingly, hacking in Sweden is a comparatively rare occupation, with no recorded prosecutions for the offence in its own right.

Those cases which reach the courts are usually prosecuted under the country's theft or economic crime statutes, usually for stealing electricity or telephone charges.

The older of the two youths, apparently aged 17 when he committed the offences, was known to the police owing to his involvement in another unauthorised system entry case dating from 1997, in which an older man was sent to jail under the economic crimes statute.

Bank in bid to catch blackmailing hacker

A German bank is offering a reward in an attempt to track down a hacker who claims to have already raided huge sums from customers' accounts.

Noris Verbraucherbank has announced it is offering a DM 10,000 (US$5,300) reward for information leading to the arrest of a hacker who the bank says is trying to blackmail the Nuremburg headquartered former private German bank.

The bank, which has gained a significant following in German online banking circles, has apparently been asked for one million DM (US$530,000) after the unknown hacker claimed to have gained access to several customer accounts and taken DM 500,000.

Bank staff are currently checking to see whether his claims to have raided customers accounts are true. In the meantime, the bank has issued its DM 10,000 reward statement.

The hacker may yet meet his downfall, however, as the bank claims his picture has been taken while he used a bank ATM earlier this month and this was recently published in a national German newspaper.

It is thought that this is Europe's first case of electronic bank blackmail, and the hacker, who apparently has not named himself, claims to have broken into the computer systems of at least two branches of the 70 branch bank.

Sources suggest that, if the money is not paid, he will publish customer information, including bank access codes, on the Internet.

In the short term at least, the incident could have serious repercussions for the German banking industry, where current legislation prevents most banks from opening outside of office hours, with the result that many Germans conduct their banking business via ATMs and online.

If the hacker succeeds, confidence in online banking in Germany could be shaken severely.

The Journal understands that police are questioning members of the infamous Chaos Computer Club over the affair (see the December 1997 issue of the Journal).

The bank's Web site is http://www.norisverbraucherbank

Pirate music Web sites told to stop

The first Internet music pirates to be sued have settled their cases after federal court action in the US.

Three defendants, who have not been named, have agreed to no longer offer free downloads of music from hundreds of artists and to destroy any unauthorised recordings on their Web sites.

The case was brought by the Recording Industry Association of America and the defendants were sued in federal courts in New York, southern California and Texas last June.

Their Internet service providers co-

News

Net thieves blocked by new law

A new law in the US aims to combat those who steal copyrighted material which has been put onto the Internet.

President Clinton signed the No Electronic Theft Act to give works the same protection in cyberspace as they would get in the real world.

The Act makes it a crime to possess or distribute multiple copies of online copyrighted material, for profit or not and penalties include fines of up to $250,000 and five years in prison.

It closes a loophole in criminal law that had allowed the distribution of copyrighted material as long as the person in question didn't seek profit.

NET Act sponsor Rep Bob Goodlatte said: "Today is a major victory for the creative minds in America who produce the music we listen to, the books we read, and the movies we watch. Copyrighted works will now be as safe online as they are on Main Street"

The Act, HR 2265, amends Federal copyright law to define "financial gain" to include the receipt of anything of value, including the receipt of other copyrighted works.

It also sets penalties for "wilfully infringing a copyright by reproducing or distributing, including by electronic means, during any 180-day period, one or more copies of one or more copyrighted works with a total retail value of more than $1,000."

The Internet, Goodlatte said, "offers tremendous opportunities. Its true potential, however, lies in the future, when students and teachers can access a wealth of high quality information through the click of a computer mouse, and business can bring the benefits of electronic commerce to consumers."

He added: "But before this can happen, creators must feel secure that when they use this new medium, they are protected by laws that are as effective in cyberspace as they are on Main Street."

Under the Act, the statute of limitations for criminal copyright infringement is extended from three to five years, and amends federal criminal code provisions regarding criminal copyright infringement to provide for a fine and up to five years' imprisonment for infringing a copyright "for purposes of commercial advantage or private financial gain, by reproducing or distributing, including by electronic means, during any 180-day period, at least ten copies or phonorecords of one or more copyrighted works which have a total retail value of more than $2,500."

The NET Act, Goodlatte said, clarifies that "when individuals sell pirated copies of software, recordings, or movies, or intentionally take pirated works and distribute them to others even if they do not intend to profit personally, such persons are stealing."

Goodlatte said the NET Act "gives law enforcement the tools it needs to bring to justice individuals who steal the products of America's authors, musicians, and software producers," while at the same time promoting "the dissemination of creative works online."

BSA settles action

The Business Software Alliance has announced that it has reached a settlement of software infringement claims against two firms in Hong Kong.

New World Infrastructure Ltd, and New World Development (China) Ltd have come to an agreement after months of legal wrangling over claimed illegal copies of Microsoft and Lotus programs.

According to the BSA, the record number of campaigns, tip-offs, raids, legal actions and settlements in 1997, clearly show that Hong Kong remains a haven for software piracy in the workplace, as well as retail piracy.

BSA vice president Tom Robertson said: "It simply makes no sense for these companies to indulge in such bad business practices.

"I'm sure that reputable companies like these would not think of stealing computers or office copiers for their internal operations - end-user software theft in the workplace is no different."

In 1997, a total of 18 cases have been settled and a total of HK$5,840,000 recovered from organisations found to have been using unauthorised software, with the single largest settlement to date of HK$1.5 million.

The recovery amount includes the purchase price of replacement software, agreed costs and damages.

Meanwhile, the territory's new Copyright Ordinance, which came into force last June, contains several important new provisions strengthening the Hong Kong Customs & Excise Department and the ability to fight software piracy.

Limiting personal information

The US government is warning Internet Web sites about collecting personal information from children.

The Federal Trade Commission's Bureau of Consumer Protection said that data should not be taken without parental consent and without allowing parents to control how the information is used.

Jodie Bernstein, director of the Bureau, said: "Any company that engages in deceptive or unfair practices involving children violates the FTC Act.

"The FTC can bring legal action to halt such violations and seek an order imposing restrictions on future practices to ensure compliance with the FTC Act."

Bernstein's announcement was accompanied by the results of an FTC "snapshot survey" of 126 Web sites on Oct. 14 that found 86 per cent were collecting names, e-mail and postal addresses and telephone numbers.

Fewer than 30 per cent collecting the data posted either a privacy policy or a confidentiality statement and only four per cent required parental authorisation before collecting the information, the commission said.

The FTC has not issued regulations on advertising for children over the Internet and other online services, but it released an "opinion letter" in July that states the agency's jurisdiction over deceptive market practices extends to the international computer network.

Although the FTC has not ruled that the web sites have broken federal law, Bernstein said the sites will be sent warning e-mail messages telling them about the problems of collecting information from a child.

Bernstein noted the Internet industry has proposed self-regulatory guidelines

to govern the collection and use of children's information and added, "This survey 'snapshot' demonstrates that these guidelines need to be more broadly implemented."

The FTC said it plans a systematic review of Internet information-collection practices in March for a report to Congress on the extent to which Internet sites, including children's sites, are posting privacy policies.

● According to reports, fourteen companies known to broadly disseminate personal information as part of their business operations across the Internet agreed to voluntarily limit access to their stored data. The move could be a pre-emptive act to avoid future legislative investigations.

It is thought the "look up" companies account for about 90 percent of the personal information distribution taking place on the Internet.

Involved in the agreement are Acxiom Corp, CDB Infotek, DCS Information Systems, Database Technologies Inc. Equifax Credit Information Services Inc, Experian, First Data Solutions Inc, Information America Inc, IRSC Inc, Lexis-Nexis, Metromail Corp, National Fraud Center, Online Professional Electronic Network and Trans Union America Corp.

The agreement calls for limiting access to Social Security numbers, dates of birth, unlisted telephone numbers and mother's maiden name, while information contained in publicly available documents such as marriages and divorces continue to be more available.

According to reports, banks, law-enforcement agencies, law firms and other businesses still have full access.

Porn detector program

A German government employee has developed a software that can detect child pornography stored on a personal computer.

The program, developed by an employee of the Hessen state criminal investigator's office, seeks out known picture information that can be downloaded from the Internet.

State government officials said the software has drawn strong interest after it was shown at a recent international police convention on child pornography in Budapest.

The system may also be useful among Internet providers seeking to find child pornography sites, the state government said in a statement from its Wiesbaden capitol.

Computer crime explosion

Australian industry is being threatened by a boom in white collar computer crime, according to a new survey.

The first study of its kind in Australia shows that three in five Australian companies have suffered some form of unauthorised use of computer systems in the past year.

Of the 300 businesses surveyed, 77 per cent reported each offence cost them $10,000, with nearly a quarter indicating six or more incidents. Six per cent of companies reported losses of more than $100,000.

Conducted by The Office of Strategic Crime Assessments and Victorian police, the Computer Crime and Security Survey also showed that banking and financial institutions were the hardest hit.

More than half (57 per cent) of businesses in the sector experienced incidents of unauthorised computer access, copying or damage to its data or programs.

The trend was "directly related to the fact that these industries have one of the highest dependencies on computers in the workplace", said researchers.

And the banking industry was followed by technology (55 per cent), communications (50 per cent) and computing (45 per cent).

Nearly 90 per cent of those surveyed traced the problem to people with legitimate access to computer systems such as trusted or disgruntled employees, contractors or consultants.

However, the trend where outsiders or hackers were intruding was also on the rise.

The survey said that similar studies in the UK indicated an escalation of white collar computer crime of around 200 per cent over the past two years and that British authorities had detected some incidents costing companies in excess of $1.5 million.

Sweden changes tack on child porn

The Swedish government has announced plans to amend its constitution to outlaw child porn of all types.

At the moment, the plans are at the proposal stages, but call for the possession, procurement, import, or export of child pornography using whatever means available, including the Internet, to be outlawed from January 1, 1999.

By amending the constitution the government will make it very difficult for future governments to change the law back without a full vote by the Parliament and a general election.

The legislation will also specifically outlaw computer generated child pornography, including images created wholly by computer.

Although possession of child pornography is not currently a crime in Sweden, government officials say they plan to match even the toughest country against the problematic material.

The Swedish government plans to hold a Parliamentary vote this spring on the issue, followed by a clause in the general election in September.

Pirate watchdog wants help from Net

The Software Publishers Association has invited Internet firms to work alongside it in clamping down on theft.

It wants to aim at tackling piracy from FTP sites, IRC channels and Usenet newsgroups and has issued an open invitation on the Web to get suggestions.

Sandra Sellers, SPA vice president of intellectual property education & enforcement said: "For some time now, SPA has been proactively filing lawsuits for copyright infringement on the Internet as part of our ongoing Internet Anti-Piracy Campaign.

"Our actions have coincided with the burgeoning growth of the Internet as a communications channel. By working

operated with the investigation and were not named in the suits.

The operators also agreed to damages of more than $1 million each, which the trade group will not collect as long as the offences do not take place again.

"The RIAA has drawn a line in cyberspace," says Hilary Rosen, RIAA president. ''People are now on notice that their actions may have serious consequences.''

Sites pirating popular tunes have been an increasing industry problem in the last year.

Powerful networked computers on university campuses and a large population of music-loving students pose a particular threat, according to the RIAA, which started an educational campaign on artists' rights.

Brent Britton, a San Francisco attorney specialising in technology issues, called the settlement ''100% in keeping with copyright law.

Plenty of people think that because it's now easy to copy and . . . distribute other people's content, it should now be legal. But the law hasn't changed. You copy, you infringe.''

Rapist bragged online

A US night club singer is wanted for rape charges after allegedly bragging online about having sex with a four-year-old girl.

David Robert Blaylock, 55, was charged with 10 counts of rape after a couple in Fort Worth, Texas, gave police copies of what they said were e-mail messages and Internet chat room conversations with him.

Blaylock fled after State Police issued a news release, and law officers were searching for him.

Police in Fort Worth said that after the couple first contacted them, they asked them to continue communicating with the man so investigators could identify him.

Sheriff Ray Byrd said that in those conversations, the man used the names "King David," "Daddy 4 You" and 'Man of Song," and eventually gave his chat partners a telephone number.

The man is accused of raping the youngster over a two-year period.

China clamps down on Internet

The government in China has announced sweeping new controls on the Internet because of fears that the network was being used to leak state secrets and spread "harmful information."

Regulations unveiled by Assistant Minister for Public Security Zhu Entao cover a wide range of crimes, including leaking state secrets, political subversion and spreading pornography and violence.

The rules are also designed to protect against computer hacking, viruses and other computer-related crime.

They call for unspecified "criminal punishments" and fines of up to 15,000 yuan ($1,800) for Internet providers and users who violate the rules, including both individuals and businesses.

One article says the Internet must not be used to "split the country," a clear reference to separatist movements in Tibet and the Moslem region of Xinjiang.

Another on "defaming government agencies" appears designed to combat use of the Internet by dissidents. A number of Chinese political exiles have home pages, which they use to attack the Beijing government.

The regulations explicitly cover information circulating from Hong Kong, Macau and Taiwan. Hong Kong reverted to Chinese rule this year and Portuguese-run Macau will be handed back in 1999. China regards Nationalist-ruled Taiwan as a rebel province.

Zhu told a news conference that Internet links since 1994 had boosted China's cultural and scientific exchanges with the world, but feared there were adverse side effects.

He said: "The connection has also brought about some security problems, including manufacturing and publicising harmful information, as well as leaking state secrets through the Internet."

Zhu said that the regulations would "safeguard national security and social stability" and added: "The safe and effective management of computer information networks is a prerequisite for the smooth implementation of the country's modernisation drive."

The regulations, contained in 25 articles, were approved by the State Council on Dec 11 and have now taken effect.

They go beyond earlier provisional regulations first promulgated in February 1996 and revised in May 1997, which also ban pornography and warn against leaking state secrets.

Chinese authorities have made attempts to censor pornography, politics and Western news organisations on the Internet. But with scores of providers, Chinese surfers have been able to find almost anything they want and it is thought that more than 49,000 host computers and 250,000 personal computers are connected to the Internet.

It was not immediately clear whether Beijing would devote more resources to policing the Internet now that new regulations were in place.

Under the new regulations, Internet providers are subject to supervision by Public Security officials and would be required to help track down violators.

● Hong Kong Internet surfers and providers will not be effected by communist China's sweeping new controls on the world-wide web, according to Anthony Wong, director general of the territory's telecommunications.

He said: "Hong Kong will regulate its own Internet and China has its own regulations.

"The regulations in Hong Kong will not apply in China and visa versa."

Wong said the Internet and telecommunications were covered by the "one country, two systems" doctrine adopted when Britain ceded Hong Kong to China in July.

Under that doctrine, Hong Kong and its 6.5 million people will enjoy a large degree of autonomy for 50 years, protecting their fiercely capitalistic ways.

Some Hong Kong users have set up Internet pages criticising China for alleged human rights abuses or policies on sensitive political issues such as Tibet.

Internet users are covered by the same rights to freedom of speech as the media in Hong Kong. The main regulations governing the Internet were laid out in an anti-crime bill passed a few years ago and focus on computer hackers, Wong said. He added: "Hong Kong has its own system, regulating its own Internet usage."

Product news

Secure electronic sales system

Hewlett-Packard and American Express said they have developed software to safeguard electronic transactions and the Web sites and databases involved in processing them.

ExpressVault software uses American Express technology to secure transactions and Hewlett-Packard's VirtualVault system to protect merchants' servers, hard drives, and Web pages.

"The combination virtually eliminates any hacking in or graffiti on a Web site," said John Galifi, American Express' electronic commerce director.

When it comes to online crime, "The big problem isn't someone trapping a single transaction," said David Alschuler, electronic commerce market research director for Aberdeen Group Inc. of Boston. It's "people invading other people's Web sites and diverting whole transaction streams."

The software, which is compliant with both the Secure Sockets Layer and Secure Electronic Transactions protocols, is to be generally available early this year.

The software is being offered through two Internet service providers, California-based Earthlink Network Inc and Mindspring Enterprises Inc of Atlanta.

Firms can buy server space from either company and can license ExpressVault for $350 a month, said Dan Abouav, director of strategic programs for Hewlett-Packard's extended enterprise business unit.

ExpressVault can accept a variety of credit cards, including American Express, Visa, and MasterCard.

Voice verification to stop phone fraud

US firms Stratus Computer Inc T-NETIX have launched voice verification technology for telephone service providers as well as commercial and financial applications.

The SpeakEZ Voice Print system works on Stratus HP-UX and Windows NT based computers.

According to the firms, voice verification can prevent wireless roaming fraud, international long-distance fraud, or agent fraud.

Corporations and financial services providers can use SpeakEZ Voice Print for a variety of security applications, such as ensuring authorised access to telephone-based financial transactions, voice mail accounts, desktop computer systems, and building entry.

The SpeakEZ Voice Print patented technology verifies a speaker's identity by matching the person's spoken passphrase with that individual's digitally stored voice print. As with a fingerprint, each person's voice is uniquely different and provides a highly reliable identification method.

Martin Mulvey, director of channel sales programs at Stratus said: "The T-NETIX solution is unique and effective, one that will enable cellular, PCS, long-distance, local, international, and other carriers to offer dependable, secure, and highly individualised telecommunications services to customers."

Richard Green, vice president of wireless at T-NETIX said: "Offering these platform options can help carriers minimise fraud costs, which is escalating into billions of dollars with today's rapidly increasing use of telco services."

The firms say the applications are vocabulary and language independent, making them easy to deploy for international use and specific applications have been developed for different market requirements.

In the wireless arena, roaming subscribers are automatically routed to a platform containing callers' voice prints, where they are prompted to say their pass phrase. If a match is made, the call goes through.

Similarly, long distance callers are routed to the platform containing their voice print, which is associated with their phone card or home phone number. After entering an ID number and speaking the pass phrase, matched-print calls proceed. According to the firms, this prevents the use of stolen calling card numbers.

For PBX security in a corporate environment, remote users can dial in and use the system as if on the premises, using extensions or long distance features of the switch.

If a fraudulent caller tries to access the switch remotely, the voice verification system will ensure that they are denied – only legitimate users can make calls.

For more information contact Stratus on +1 508 490 6430, e-mail lynette_gutcho@stratus.com or access the firms' web sites at http://www.stratus.com and http://www.T-NETIX.com

Strong encryption export goes ahead

Computer hardware seller Cylink Corp says it has become the first hardware vendor to win US government approval to export 168-bit encryption to Europe without key recovery.

The company said the Commerce Department approval was specifically for export to European central banks, which include a network of all 15 European Union countries as well as non-EU members Switzerland, the United States, Canada and Japan.

The US government has been limiting the export of so-called strong encryption because it says companies should offer "key recovery" options that could enable government and law enforcement authorities to tap into encrypted data to decipher its contents.

The central banks have mandated use of this particular level of encryption, which scrambles and unscrambles data so it can be transmitted securely without being read by unauthorised parties.

Many companies have complained that U.S. export limits held back the development of electronic commerce over the Internet, and the government has gradually eased its policy.

"The government has taken a very positive step," said Fernand Sarrat, Cylink's president and chief executive officer. "It's the first time that you have the strongest encryption without the requirement of key recovery."

Sarrat said Cylink was the first to receive the clearance for the 168-bit encryption, known as Triple-DES (data encryption standard), without a key recovery mechanism.

Stolen computer hot list on the Net

With computers now topping the list of most-often-stolen equipment, a service to help people check up on suspect equipment is being stepped up.

The Stolen Computer Registry, a worldwide clearinghouse for serial numbers of stolen gear, is increasing its efforts to fight theft by making access to its Internet database free to all.

Operators of the service say that corporate and individual victims of computer theft, computer traders, insurance companies, law enforcement agencies and private individuals can now list serial numbers of stolen equipment and compare serial numbers of suspicious gear.

The Stolen Computer Registry has been tracking stolen gear since 1990. When stolen gear is located, the Registry assists in its recovery and return to its rightful owner.

A spokesman for the service said: "To help fight theft, stolen serial numbers should be listed immediately after a computer is stolen, and serial numbers should be checked before any used or demo computer is purchased.

"In this way, an informed public can protect itself from being used as a pawn for crooks and unscrupulous dealers."

The Registry website is located at www.nacomex.com

Stolen serial numbers can also be faxed to the Registry. Reporting Forms may be obtained by writing to Stolen Computer Registry, P0 Box 394, Tivoli, NY 12583, US, or faxing +1 914-757-4144.

Firms fail on IT security enforcement

According to a report published by software distributor Integralis, information technology managers in the UK have to step up their security measures to avoid costly problems.

The company surveyed around 100 UK users of the firm's MimeSweeper package during last month, and concluded that around 75 percent of all organisations are failing to enforce their IT security policies, leaving themselves vulnerable to security breaches.

According to the report, while 95 percent of the companies questioned have a security policy, only a quarter of them strictly enforce it.

Integralis claims that the survey highlighted the dangers that organisations face with the increase in employee access to the Internet and e-mail.

Of those firms questioned, nearly 80 percent have Web enabled desktops and allow their staff personal use of electronic-mail systems. This freedom of access, company officials said, continues to increase the threat of businesses landing in court over issues such as the spreading of libellous comments, sensitive information, or jokes in bad taste.

The survey polled staff working at a total of 60 organisations, each with a minimum of 500 e-mail users and concluded that senior managers have been slow to recognise the value of content security as well as access security.

Only 57 percent of IT managers polled claim that this is taken seriously by their bosses, despite the growing emergence of content-based security threats, the report noted.

These include junk mail, hidden viruses, Java applets, and ActiveX, time-wasting on the Web, and e-mail, confidentiality and liability issues.

According to Chris Hislop, Integralis' marketing manager, the figures from the report support the feeling amongst IT departments that content security is every bit as important as access security.

He said: "A flexible content security solution can offer organisations protection against a number of threats not covered by access security alone."

Integralis' Web site is at http://www.integralis.com

Fingerprint leads to gang busting action

A single fingerprint taken from the scene of a vicious fight became the key to ending a bitter turf war in Montreal, Canada.

Rival motorcycle gangs were terrifying the people in the city, with random shootings and bombings, including the car bomb death of an innocent 10-year-old boy.

According to Printrak, maker of electronic fingerprint systems, the vital print was found in a stolen van that had been used to commit a homicide.

It was developed and electronically transmitted to the Royal Canadian Mounted Police central Automated Fingerprint Identification System and was identified within an hour.

The homicide was regarded as a professional hit and possibly gang-related and investigators put the subject under surveillance.

And when the subject was arrested, detectives learned of his plans for another murder. After being confronted with the evidence of the latent fingerprint identification, the subject agreed to become an informant.

He admitted that he was a contract killer and agreed to testify against the gang. He was eventually convicted of five counts of murder, 13 counts of conspiracy to commit murder and various weapon offences. His testimony aided in the arrest and conviction of numerous gang members.

William Whyte, chief superintendent, RCMP said: "The impact of automated fingerprint identification is clearly illustrated by this dramatic situation. One AFIS identification crippled a well-organised crime ring. One ID helped to cage ruthless and vicious killers."

In the law enforcement arena, such identifications are known as "hits." The Canadian case was singled out as "Hit of the Year" at the Printrak International 19th Annual Users' Conference held in California, which was attended by nearly 300 officials and administrators from around the world.

Contact Printrak on +1 714 238 2000

Testing time for anti-virus software

Virus Bulletin magazine has announced a new award scheme to find the best anti-virus programs on the market.

It says it will put the products through a stringent testing procedure using the most recent wild list of viruses and those

Court reports

that have a 100 per cent detection rate will get a VB mark of approval.

Editor of Virus Bulletin Nick FitzGerald said: "There is no charge for certification and the associated logo earned by a product scoring 100 per cent will clearly state the product, platform and date of award. This allows purchasers to see through marketing tricks such as using outdated awards in packaging artwork and literature."

For more information contact Virus Bulletin on +44 1235 555139 or e-mail subscribe@virusbtn.com

Finding missing kids using the Internet

Non-profit organisation ANSER in the US has won an agreement worth $3.5 million from the National Institute of Justice to develop a system to help missing children.

The system will also be used on other networks as well as computer databases of information, photos, and video to improve public safety by integrating intelligent software agents and facial recognition technology to search, access and report relevant information about missing children.

Its first application is for the National Center for Missing and Exploited children to assist case managers to search the Internet for relevant information and obtain possible facial matches of missing or exploited children.

Developers say the goal is to create intelligent software agents that can be trained to prioritise information and anticipate user needs.

These intelligent software agents will perform tasks currently done by humans, thus automating the investigative processes. The system will be further developed for additional law enforcement applications.

Dr Helena Wisniewski, ANSER vice president, information technology, said: "It is rewarding to see how technology, that is useful to business and corporate growth, can also benefit the public good."

For more information, contact ANSER on +1 703 416 3505 or visit the Web site at http://www.anser.org.

Man jailed after Net sting

A New York man has been jailed for 15 months after he travelled across state lines to meet who he thought was a 13-year-old girl he met over the Internet.

Carmine Iommazzo, 31, of New Rochelle, pleaded guilty to travelling from New York to St. Petersburg, Florida, to meet with a girl he believed was named Casey Lee Givens. He was sentenced by US District Judge Barbara Jones in Manhattan federal court.

Givens was actually an undercover detective with the St Petersburg Police Department who signed on to America Online using the screen name "Caseylee13" and posed as a 13-year-old girl.

According to the complaint, Iommazzo, who used the screen name "Takeme100," discussed "graphic sexual matters" with Givens during online chats and he arranged to meet the ficticious girl at a St Petersburg park in August 1996.

After meeting with the undercover officer, Iommazzo was arrested and charged under Florida law with attempted lewd and lascivious acts with a minor under the age of 16.

At the time of his arrest, he admitted that he had about 50 child pornographic computer image files in his home computer and the age range of the children ranged from six to teens.

Judge freezes assets of alleged fraudsters

Two companies and their presidents, accused of using the Internet to defraud investors in a $20 million Ponzi scheme, had their assets frozen by a federal judge, the US Securities and Exchange Commission said.

US District Judge David Sam in Salt Lake City granted a temporary restraining order for Capital Acquisitions Inc. and its president, Wayne Notwell, and Somerset Group Inc. and its president, Clealon Mann, all of Salt Lake City, the SEC said.

The order stemmed from the commission's civil complaint that Capital allegedly raised about $20 million from at least 600 investors nationwide, beginning in 1996, through sales of three-year notes offering an annual "guaranteed" return of 20 percent, the agency said.

Investors were solicited through a network of sales agents directed by Mann and Somerset, the agency said in its complaint. At least one of those agents posted the offering on the Internet, which led to its detection by the SEC.

In the civil complaint, also filed on Dec. 19, the SEC alleged the defendants defrauded investors by conducting a Ponzi scheme, with the source of the promised interest payments being funds received from the ongoing sale of Capital's notes, the agency said.

A Ponzi scheme is a fraudulent pyramid-type scheme in which investors seeking high interest-rate returns are lured and earlier investors are paid off with funds from newer investors.

Attorney vows to get tough

After the conviction of a man on federal child pornography charges, US Attorney Karen Schreier said her office will clamp down on Internet crimes.

Schreier said the conviction of Jack Chew, 54, is the first of what she believes will be many prosecutions for offences committed over the Net.

Chew, a used car salesman from St. Joseph, Missouri, was convicted of transporting child pornography across state lines. He could be sentenced in March to 15 years in prison and fined $250,000.

Chew had brought his computer to a company in Sioux Falls for repairs when more than 150 pictures of naked children, some engaged in sex acts, were discovered.

He claims he was trying to find out where the pictures came from so he could stop the spread of pornography. And Chew said the pictures did not exist because his computer was broken when he shipped it to South Dakota. Schreier said her office has five people under indictment for child porn on the Internet.

Internet crime can be easy to prosecute because material clearly crosses state lines, breaking federal law, she said.

US technology bills

Congress faces major computer legislation issues for 1998

This year the US legislative machinery has a number of bills and hearings scheduled to deal with a host of controversial high technology issues.

- On the international front, two encryption related bills, H.R. 695, the Security and Freedom through Encryption (SAFE) Act, and S. 909, the Secure Public Networks Act, remain stuck in the House of Representatives' Rules Committee and the Senate Commerce Committee, respectively.

The SAFE Act, which would allow US manufacturers to freely export encryption products, and sponsored by Rep. Bob Goodlatte, has run aground in the House Rules Committee due to the insistence of Chairman Gerald Solomon to include amending language.

The proposed amendment would make it unlawful for any person to manufacture, distribute, sell, or import into the US any encryption products that do not allow "immediate and surreptitious access by law enforcement".

The amendment also would require all network service providers offering encryption products or services, from telephone companies to Internet service providers, to ensure that each message can be immediately decrypted without the knowledge or co-operation of the user.

- The Secure Public Networks Act of 1997, introduced June 16 and sponsored by Senators John McCain and Bob Kerrey, has been referred to the Senate Commerce Committee, with no action scheduled.

This encryption bill was introduced as a compromise to Goodlatte's SAFE Act, and is intended to strike a balance between the needs of law enforcement and industry concerns, framed around the Clinton administration's encryption policy.

It includes a complex mandatory key recovery scheme, but has yet to be discussed or amended in committee to date.

- On the copyright front, S.1044, the Criminal Copyright Improvements Act of 1997, is awaiting action by the Senate Judiciary Committee. The bill will amend the Copyright Act, closing the "LaMacchia Loophole" by enabling law enforcement to prosecute commercial scale Internet software pirates for criminal copyright infringement even in the absence of commercial gain.

- H.R. 2281 and S. 1121, the World Intellectual Property Organization (WIPO) Copyright Treaties Implementation Act of 1997 is continuing through hearings in House Judiciary subcommittee on courts and intellectual property.

The bill will make necessary amendments to US law to enable the Senate to ratify new international intellectual property treaties negotiated last year in Geneva. Efforts by telephone company interests to gain exemptions from liability from copyright infringement on the Internet have slowed its progress in both chambers.

- The Software Trade Secrets Protection Act of 1997, H.R. 2667, passed the House Ways and Means Committee October 21. The bill will curb unnecessary intrusions by the Internal Revenue Service into the intellectual property of software companies. The IRS has begun issuing subpoenas to access source code of tax preparation software while conducting routine audits of multinational companies.

- S. 442 and H.R. 1054, the Internet Tax Freedom Act of 1997, sailed through the full US Senate Commerce, Science and Transportation Committee by a three to one margin, clearing the way for a full Senate vote. The Committee passed a substitute amendment to the Internet Tax Freedom Act, S.442, by a 14-5 vote. The amended bill would create a national policy against state and local government interference with interstate commerce by establishing a six-year moratorium on state and local taxes on Internet access services, online services, and communications or transactions using the Internet until January 1, 2004.

Bill co-sponsor Ron Wyden said he was optimistic the bill would pass the full Senate early next year.

The House version of the bill, H.R. 1054, is waiting for the full House Judiciary and Commerce Committees to approve the bill and move it to the House floor.

- A "spam ban," introduced by Rep. Christopher Smith is making the rounds through Congress. The Netizens Protection Act of 1997, designed to ban the unsolicited commercial e-mail inundating electronic mailboxes, would include all unsolicited commercial e-mail, including get-rich-quick schemes, electronic dating services, offers of unproved medical remedies, and other solicitations that ultimately cost consumers in online charges, unlike regular junk mail.

The bill, Smith said, "will help people not only with the nuisance of spam but the costs as well." And he added that anyone wanted to continue to receive spam mail could do so under the Netizens Protection Act.

The House is expected to re-examine Smith's bill earlier this year.

International summit

In one of the most important developments in the fight against computer crime, eight of the most powerful countries have got together to discuss the problem and identify solutions. The findings will be important to everyone in the field of forensic computing, reports **Paul Johnson**.

Senior politicians from the Group of Eight claimed they laid the groundwork "for the next century of crime fighting," when they met for the first ever conference of its type.

Justice and Interior Ministers and Deputy Ministers from the countries, made up of the G7 states and Russia, met in Washington DC in the US in an attempt to reach a number of agreements to thwart the growing network of computer-based criminals across the globe.

The Group of Eight's two-day meeting, which included representatives from the US, the UK, France, Germany, Italy, Canada, Japan and Russia, covered the range of computer crime issues, from education to data security to harmonising individual legal systems to ensure prosecution.

US Attorney General Janet Reno, leading the discussions, said: ""If we are to keep up with cybercrime, we must work together as never before.

"Criminals no longer are restricted by national boundaries. We know now that a criminal can sit in one country and disrupt a computer system in another country thousands of miles away.

"For instance, we know now that a criminal can sit in one country and disrupt a computer system in another country thousands of miles away.

"Twenty-first century technologies are going to change how we live, and make many things easier, but computers and networks are also opening up a new frontier of crime.

The group agreed on a general plan that includes more computer training for law enforcement personnel in each country and the establishment of high-tech contacts that will be available to officials in each country on a 24-hour basis.

Each nation committed to develop faster ways to trace attacks coming through computer networks and to devote more time and resources to crimes committed by international criminals who escape extradition.

"This agreement applies not just to computer crimes, but to all types of otherwise extraditable crimes," Reno said.

Computer criminals are harder to track because networks allow anyone to reach into computers around the world inexpensively and often anonymously, said Scott Charney, chief of the Justice Department's computer crime and intellectual property section.

"As a result, people who are interested in doing criminal things can attack computer systems from anywhere in the world and use computer systems to facilitate traditional offences, like distribution of copyrighted material or child pornography," he said.

The ministers committed to "ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of fighting high-tech crime," Reno said.

And the group also agreed to establish high-tech crime contacts available on a 24-hour basis.

"This will enable us to more immediately track down computer criminals or lend other critical support," Reno said.

The eight world leaders also plan to develop faster ways to trace attacks coming through computer networks, to quickly identify hackers or criminals responsible for the attacks.

Reno said the group also plans to plug extradition loopholes. "Where extradition of a criminal is not possible because of nationality, we will devote the same commitment of time and resources to that prosecution that a victim nation would have devoted," she said.

"This is important because too often, a criminal will flee a country and return to his or her own homeland, hoping to escape justice if extradition is not possible."

Reno added that this commitment would apply not only to computer crimes, "but to all types of otherwise extraditable crimes."

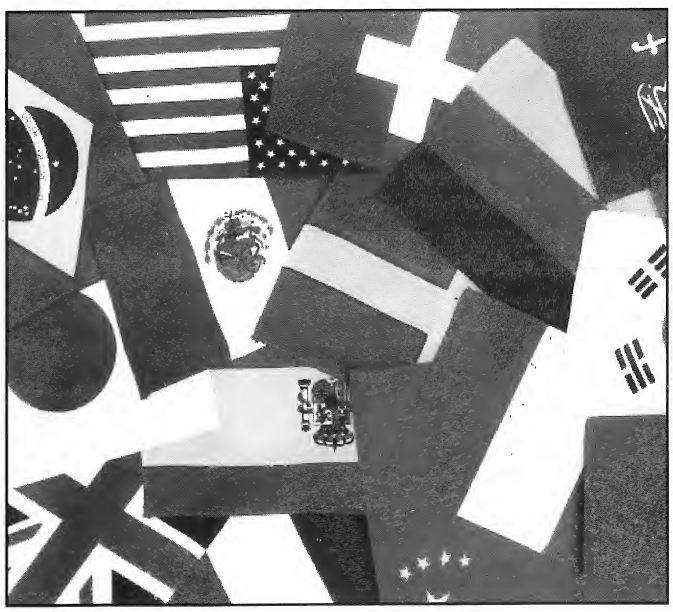
Noting how computer criminals in one country can alter or destroy electronic evidence before enforcement in another country can act, Reno said the group plans to take steps aimed at preserving information on computer networks.

"In taking this step," she said, "information will be less likely to be tampered with by criminals, or erased by routine system update procedures."

The ministers also agreed to review each country's legal systems "to ensure they appropriately criminalise computer wrongdoing and ensure they facilitate the investigation of high tech crime".

Vowing to work closely with the high tech industry to devise new solutions to detect, prevent and punish computer crimes, Reno said the group plans to "intensify our efforts to use new technologies," including the use of video links.

"Video links will enable us to obtain testimony from witnesses located thousands of miles away," she said. "With



emerging technologies, no longer will we have to fight 21st century crimes with 19th century tools."

The meeting also called for the development and employment of "compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions".

Jack Straw, the British home secretary, said the steps would be of "major importance" in attacking cybercrime. "The challenge is from moving one step behind these criminals to being one step ahead," he said.

Straw also recommended a closer dialogue with Internet service providers so they become aware of the needs of law enforcers. He said that ISPs are more independent and entrepreneurial than the major long-established telecommunications companies, which are often state-owned or regulated.

He said: "We need a closer dialogue so they are aware of our needs, and so they recognise we are all on the same side."

Officials said Internet services could aid authorities most by helping identify those rogue clients faster. But service providers said that they must respect the privacy of their clients and that enforcement should be left in the hands of investigators.

''It's not our job to police the Internet,'' said Dennis Spina, chief executive officer of Erol's, a Virginia-based provider. ''But we notify the authorities when we become aware that something has gone wrong.''

Mark Rasch, a lawyer with Science Applications International Corp., said, ''Service providers want to be good partners, but they shouldn't be required to do more than anybody else.''

No schedule for implementation of the agreement was set, nor did officials from the eight countries estimate the economic cost of computer crime.

Officials say a treaty among the European nations to combat computer crime may follow the agreement. The treaty, slated for completion by Dec. 31, 1999, is being negotiated by the European states in the multinational Council of Europe.

Full text of the agreement

At the Summit of The Eight in Denver, our heads of state and government directed us to intensify our efforts to implement the 40 recommendations of the Summit of Lyons, in order to combat transnational organised criminal activity posing an ever-greater threat.

With increased international movement by criminal groups and their use of new global communications technologies, the protection of our citizens' safety, traditionally a domestic concern, requires unprecedented levels of international co-operation. Our responsibility is not only to react to the activities of organised criminal groups, but also to anticipate and prevent their growth.

We meet at the ministerial level to agree upon a program of specific actions designed to accomplish two critical tasks, enhancing our abilities to investigate and prosecute high-tech crimes and strengthening international legal regimes for extradition and mutual legal assistance to ensure that no criminal receives safe haven anywhere in the world.

With regard to high-tech crime, we must start by recognising that new computer and telecommunications technologies offer unprecedented opportunities for global communication. As nations become increasingly reliant upon these technologies, including wireless communications, their exploitation by high-tech criminals poses an ever-greater threat to public safety. This threat takes at least two forms.

First, sophisticated criminals are targeting computer and telecommunications systems to obtain or alter valuable information without authority and many attempt to disrupt critical commercial and public systems. Second, criminals, including members of crime groups and terrorists, are using these new technologies to facilitate traditional offences.

Clearly, the misuse of information systems in these ways poses a serious threat to public safety.

National laws apply to the Internet and other global networks. But while the enactment and enforcement of criminal laws have been, and remain, a national responsibility, the nature of modern communications networks makes it impossible for any country acting alone to address this emerging high-tech crime problem.

A common approach addressing the unique, borderless nature of global networks is needed and must have several distinct components. Each country must have in place domestic laws that ensure that the improper use of computer networks is appropriately criminalised and that evidence of high-tech crimes can be preserved and collected.

Countries must also ensure that a sufficient number of technically literate, appropriately equipped personnel are available to address high-tech crimes.

Such domestic efforts must be complemented by a new level of international co-operation, especially since global networks facilitate the commission of transborder offences. Therefore, consistent with principles of sovereignty and the protection of human rights, democratic freedoms and privacy, nations must be able to collect and exchange information internationally, especially within the short time frame so often required when investigating high-tech crimes.

The development of effective solutions will also require unprecedented co-operation between government and industry. It is the industrial sector that is designing, deploying and maintaining these global networks and is primarily responsible for the development of technical standards. Thus, it is incumbent of the industrial sector to play its part in developing and distributing secure systems that, when accompanied by adherence to good computer and personnel security practices, serve to prevent computer abuse. Such systems should also be designed to help detect computer abuse, preserve electronic evidence, and assist in ascertaining the location and identity of criminals.

To meet the challenges of the information age, we have agreed to 10 Principles and a 10-point Action Plan.

We direct our experts to promote these Principles throughout the interna-

tional community and take forward the Action Plan without delay.

Another core area of concern is mutual legal assistance and extradition. We reiterate the fundamental importance of either returning our nationals for trial in the country in which the crime was committed or, where that is not possible, conducting effective domestic prosecutions in lieu thereof. Those of us that conduct domestic prosecution of our nationals in lieu of extradition agree to pursue such prosecutions with the same commitment of time, personnel and financial resources as are devoted to the prosecution of serious crimes committed within our own territory.

We recognise that the need for enhanced co-operation in extradition and mutual assistance is particularly acute with respect to high-tech crime. We commit to remove impediments in existing co-operation regimes by such means as approaching issues of dual criminality with flexibility, and we will ensure that serious computer abuses have criminal penalties to make them extraditable.

We also commit to enhance co-ordination among states in multi-jurisdictional cases, so as to minimise conflicts and duplication in investigations and prosecutions, consult as to where best to prosecute, and allocate responsibility for gathering and sharing evidence.

We are also convinced that we must further enhance our abilities to obtain testimony from witnesses located abroad for use in criminal proceedings in our states. We agree to intensify our efforts to use video-link technology as a means of securing testimony or statements from a witness located abroad. Where possible, we will locate or establish facilities with technical video-link capability, allow the use of video-link as a form of mutual assistance to other States and provide for the punishment of perjury committed during video-link transmissions.

We emphasise that these agreed-upon measures can be used by all countries to enhance international co-operation in combating transnational organised crime. Our experts will review annually our implementation at the national level of these international legal co-operation measures. We also urge all states to adopt the recommendations of the Summit of Lyons pertaining to international legal co-operation and the best practices agreed upon by our experts to implement them.

We direct our experts to focus their future work on the following areas: Continued examination of the use of video-link technology and confiscation and sharing of assets obtained through criminal activity, identification of additional measures that would enhance co-operation in areas of emerging significance, ways to further promote acceptance by other members of the international community of the principles set forth in the above recommendations and practical actions, and co-ordination among The Eight on the possible elaboration of a UN organised crime convention.

In addition to taking action on high-tech crime and mutual legal assistance, we further direct our experts to pursue their work in implementing comprehensive action against transnational organised crime, as mandated by the Denver Summit.

Therefore, we welcome the continued efforts of our experts to develop co-operative strategies and policies to combat major transnational criminal organisations and to implement joint operational projects to target such organisations and their criminal activities. We will continue to work together to combat international firearms trafficking and other forms of cross-border crime and smuggling and to address the financial aspects of organised crime.

In conclusion, we recognise the urgent need to make rapid progress in these areas and will take the steps necessary to ensure protection from the physical and financial threat of transnational organised crime.

Our task is daunting, but we expect to report substantial progress in this endeavour to the Birmingham Summit in May of 1998.

Fundamental principles agreed by summit

I. There must be no safe havens for those who abuse information technologies.

II. Investigation and prosecution of international high-tech crimes must be co-ordinated among all concerned States, regardless of where harm has occurred.

III. Law enforcement personnel must be trained and equipped to address high-tech crimes.

IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorised impairment and ensure that serious abuse in penalised.

V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.

VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorisation from the State where the data resides.

VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.

IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

X. Work in this area should be co-ordinated with the work of other relevant international groups to ensure against duplication of efforts.

Case study

Trade secrets - finding the evidence

This case study summarises an investigation into a senior employee of a high-tech company who was apparently passing trade secrets to the competition. The investigation focused on gathering evidence that proprietary data was transferred via e-mail or on floppy disks.

The suspicion

Company A, which produces design software for architects, identified that Company B, one of its competitors, appeared to be releasing similar software and was successfully selling into Company A's client base who had previously been loyal to Company A.

As a result of a brief internal investigation it was established that one of the senior executives at Company A was disillusioned with his career and was potentially seeking employment with Company B.

Company A was unable to ascertain whether this senior executive was providing the competitor with proprietary information as there were no hard copy documents pertinent to the investigation in the senior executive's office and the information that was suspected of being stolen was design software and client details in a database.

Copying Procedures

The investigation brief was to covertly examine the contents of a laptop computer used by the senior executive and a desktop computer used by his secretary. Any floppy disks found in the office were also to be examined.

The desktop computer was easily accessible and was copied to an optical cartridge. This was then used to re-create an exact copy of the original hard disk onto a working hard disk. All subsequent examination was carried out on the reconstruction, thus preserving the evidential integrity of the original optical disk copy.

The floppy disks were write protected and then copied to image files on an optical cartridge using dedicated forensic software. All examinations were carried out on the image copies.

The laptop used by the senior executive was always on his person and could not be examined in the initial stage of the investigation. When examined at a later stage the same copying procedure was used as for the previous desktop.

Examination of the desktop

On examination of the desktop it immediately became apparent that there had been some non-standard interference with the system prior to copying.

Enquiry revealed that the IT department of Company A had removed the desktop on the night prior to copying. When questioned they somewhat reluctantly admitted that they had tried to view active files and undelete deleted files.

They had found nothing. They had not considered the risk that undeleting files would overwrite potentially helpful evidence nor that they had invalidated the evidential integrity of the machine.

In the event it was fortunate that the investigation of the desktop did not reveal any useful evidence and the disruption of the evidence by the client did not damage the enquiry.

Examination of the laptop

On the evening of the investigation all laptops were recalled by the IT department to "install new virus check software" and the laptop belonging to the senior executive was intercepted.

It was ensured that on this occasion the client had no opportunity to attempt an in-house investigation.

The client was anxious for a rapid response and, therefore, a quick analysis of the operating environment on the laptop was performed. This established that the laptop's hard disk had two partitions, one running a Windows 95 operating system, the other running a Solaris Sun operating system.

A review of the file lists in the applications indicated that the user had apparently been working on documents saved to the A:\ drive recently and the cache directory indicated that the user appeared to be an active Internet user.

These findings suggested that it would be beneficial to perform a detailed investigation searching for evidence that proprietary files and/or data had been copied off the laptop or the company server onto floppy disk or had been sent out via e-mail.

A low level search was performed using the DIBS® Computer Forensic Searcher module (a non discriminatory search engine) for strings including various different segments of e-mail ad-

dresses, Company B's name and its officers' names and the string "A:\". Although the search was across both partitions the majority of useful hits were found to be in the Windows 95 partition.

The Findings

An investigation of the clusters containing hits revealed many fragments of incriminating e-mails that contained text referring to the content of attached documents that indicated the documents contained proprietary information.

It appeared that some of the e-mails had been sent to individuals at Company B. It was also possible to establish that there had been a considerable amount of recent activity saving information to the A:\ drive, including saving documents titled "CV.DOC", "BUSPLAN.DOC" and "BUSPLAN1.XLS".

There were no files on the laptop hard disk that matched the above file names. However, deleted files were identified called "åV.DOC", "åUSPLAN.DOC" and "åUSPLAN1.XLS". We were able to recover two of these files which indicated that the senior executive was seeking employment with Company B and that he appeared to have plans to launch a similar product to Company A's when with his new employer.

Conclusions

As is often the case, the client attempted to investigate the suspect computers directly which damaged the evidential integrity of the findings.

In this case however it was fortunate that they only had access to a peripheral machine and they had no access to the computer that yielded the critical evidence.

The investigation produced sufficient evidence for the employment of the senior executive to be terminated and for an agreement to be reached whereby the executive was restrained from interacting with Company B and a significant sum was paid to Company A in compensation.

By **Mark Taylor**, Computer Forensic Investigations Ltd.

The firm can be contacted by e-mail at info@computer-forensic-inv.com

Two men are being charged in separate cases in the US with sabotaging company computer networks.

George Mario Parente is accused of damaging computer data at new York magazine publishing company Forbes Inc and Senal Arabaci is alleged to have hacked into Art Assets LLC, an art seller and distributor.

According to US Attorney for the Southern District of New York Mary Jo White, Parente and Arabaci are being charged in separate complaints "with knowingly causing the transmission of a command, and as a result, intentionally causing damage without authorisation to a computer which is sued in interstate commerce."

The complaint against Parente alleges the ex-Forbes computer technician hacked his way into Forbes Inc.'s network in April, 1997, from his residence using a modem and an unauthorised password. Once online, Parente caused a massive crash of Forbes' computer network in New York City, resulting in damages in excess of $100,000, the complaint charged.

The complaint against Arabaci, a former computer contractor for Art Assets LLC, charged that Arabaci deleted and modified Art Assets' files and databases, causing a loss in excess of $10,000. The Parente complaint noted that Parente dialled into Forbes' computer network by signing on under the identity of a former colleague at Forbes that Parente was not authorised to use.

While connected to the Forbes network, Parente caused "a massive system crash to occur," the complaint said, leaving five of the network's servers inoperable. Parente's calls, however, were traced back to his unlisted home phone number by Forbes' computers.

Agents from the FBI's Computer Crimes Squad conducted a court-authorised search of Parente's residence in Howard Beach in the New York City borough of Queens. They seized, among other things, computer disks containing articles about computer hacking and sabotage, computer viruses and hackers' tolls, including Trojan horses that are used to sabotage computer networks, and "various items of confidential and sensitive business information on Forbes."

One document found in Parente's residence, the complaint said, was "The Complete Social Engineering FAQ (frequently asked questions)" which describes the "aim" of social engineering as "(tricking) people into revealing passwords or other information that compromises a target system's security."

Parente was released by US Magistrate Douglas Eaton on $50,000 bond after Parente made an initial court appearance. According to the Arabaci complaint, Arabaci, who lives in Manhattan, had been the administrator of all user accounts at Art Assets, and had access to all user names and passwords.

On August 19, 1997, several weeks after Arabaci completed an assignment to implement Art Assets' computer network, Arabaci met with several Art Assets' personnel to attempt to resolve a billing dispute, the US Attorney's office charged.

During this meeting, the complaint said, one of the owners of Art Assets criticised Arabaci's technical abilities, telling him, in substance, "that he had done a poor job installing the Art Assets network."

According to the complaint, Arabaci logged into Art Assets' computer network on the evening of the August 19 meeting, and "deleted and modified files and databases."

"Computer networks are vital to our economy and our safety," US Attorney White said, "and their security should be one of law enforcement's and industry's highest priorities."

Noting that "too often computer crimes are not reported to the authorities," White said the victims in these cases, Forbes and Art Assets, "should serve as role models for the business communities of America."

"Businesses should work together with law enforcement to protect the integrity of the country's computer networks by reporting these crimes," she said. "Those who prey on computer networks, whether motivated by espionage, sabotage or recreation, will be prosecuted."

Each of the crimes in the two complaints carries a maximum prison term of five years and a maximum fine of $250,000.

Computer evidence

The important first step - safe seizure of the computer

By
Michael R. Anderson

It is pretty clear - the computer age has arrived and it is in full bloom. If you don't believe me, just try to find a national advertisement that doesn't prominently list the Internet web site of the advertiser.

Or try to find a business that doesn't rely on a computer to track its sales and maintain its business records. Computers are everywhere. They have even found their way into most households and portable computing is a way of life for most business travellers.

The rapid acceptance of computer technology by all segments of our society has created new and interesting challenges for law enforcement agencies and prosecuting attorneys. Computer evidence has become a 'fact of life' for essentially all law enforcement agencies and many are just beginning to explore their options in dealing with this new technology.

Almost over night, personal computers have changed the way the world does business. They have also changed the world's view of evidence because computers are used more and more as tools in the commission of 'traditional' crimes.

Embezzlements, theft, extortion and even murders are now committed with the aid of a personal computer. This new technology twist in crime patterns has brought computer evidence to the forefront in law enforcement circles.

Computer evidence concerns are not limited to computer crime specialists in the Federal Bureau of Investigation or United

States Secret Service. Every law enforcement agency now has the potential of encountering computer evidence and many are actively seeking training and information on the topic.

My hope is that this article will provide guidance and awareness to law enforcement agencies that exploring the issues surrounding computer evidence.

The article is not intended to be a substitute for training. I am aware that there is more than one way to 'skin a cat' and this information is certainly not intended to be the only 'true way'. However, the information should help law enforcement agencies get started in the right direction. It should also act as a refresher for those agencies that have experience in processing computer evidence.

Preservation of computer evidence is crucial. Computer evidence, by its nature, is extremely fragile and is easily modified.

This situation is complicated by the fact that potential evidence exists in places that many law enforcement officers are unaware of. To make matters worse, computers can easily be rigged by the 'crooks' to destroy evidence.

Some have referred to personal computers as a law enforcement nightmare and a crook's dream. Because of its fragile nature, the first and most important step in dealing with computer evidence involves the preservation of the 'electronic crime scene'.

No law enforcement professional would allow evidence to be disturbed or destroyed at a traditional crime scene. The same is true of computer evidence. However, because the nature of the evidence is different, the rules change a bit.

Assume every computer has been rigged to destroy evidence. When it comes to computer evidence, paranoia is a good personality trait to have. Don't operate a suspect computer until a complete backup has been made of all storage devices. Standard computer backups won't do and a full bit stream backup is necessary.

In the bizarre world of computer evidence, you always must assume that things will go wrong. Once computer evidence has been destroyed or altered, it is unlikely that it can ever be reconstructed.

Murphy will be looking over your shoulder every step of the way and what can go wrong surely will go wrong. Complete backups eliminate most of the potential problems.

Law enforcement officials normally seize computers during the execution of a search warrant. Depending on the circumstances and scope of the search warrant involved, all computer hardware, software and manuals should be taken for evaluation as potential evidence. Some prosecutors may view this as overly broad. However, the ability to process and examine the evidence may be directly tied to special hardware, software and/or written instructions contained in manuals.

Because computer technology changes so quickly, it may be impossible to obtain similar or outdated hardware or instruction manuals from other sources.

Printers, tape drives, optical drives, hardware manuals and software manuals should not be left behind. I have stressed this in my various training courses for years and practical experience has proven that the advice has merit.

Also, pay particular attention to possible passwords that may have been written down near the computer. Encrypted files can cause you serious grief and finding a password scrawled on a desk or on a calendar can help make your case.

More and more, corporations and government agencies are involved with computer evidence pertaining to internal investigations and internal audits.

The same law enforcement procedures should be followed by corporate

computer specialists because it is usually unknown if criminal violations are involved initially.

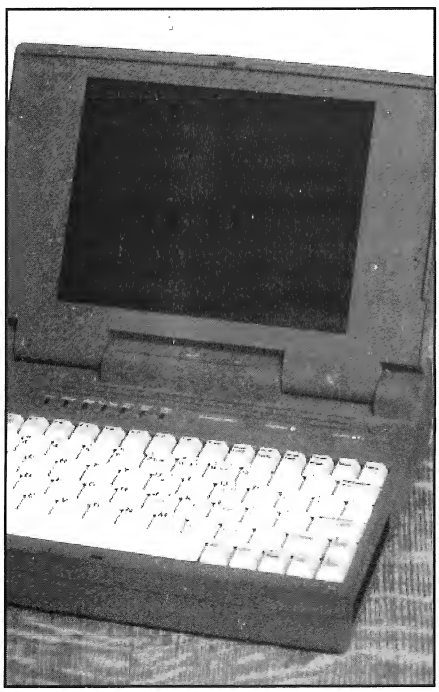
Following accepted computer evidence processing procedures will insure that the case meets the requirements for both civil and criminal trial purposes.

When we conduct corporate training courses, I stress that every case should be treated as though it will go to trial. However, some things are a bit different when it comes to corporations. In a corporate or government setting, the ability to 'seize' a computer and evaluate the data stored on the computer's hard disk drives and floppy diskettes may be ruled by corporate policy and privacy laws.

For this reason, it is essential that corporate legal counsel be consulted before taking any steps to seize or process a corporate computer.

In the absence of a corporate policy covering computer evidence and privacy issues, corporate computer specialists could be exposing themselves and the corporation to a potential law suite.

Caution should always be used in the shutdown and transport of the subject computer. To preserve the image on the screen, a quick photograph of the screen display may be appropriate. Then a decision has to be made as to whether or not the computer will be unplugged from the wall or shut down systematically, based on the requirements of the operating system.



Unfortunately, there is no correct answer and there are risks in taking either course of action. Your decision will depend on the particular facts involved, the operating system involved, and your good judgement.

In training classes, I usually recommend that networked computers be shut down following normal shutdown procedures as dictated by the operating system involved.

Usually, standalone computers can be unplugged as long as background processes are not active, e.g. disk defragmentation.

If at all possible, avoid running any programs on the subject computer. To do so can create temporary files that may overwrite valuable evidence.

Also, be careful using the keyboard to enter standard operating system commands. Even one wrong press of a key can trigger destructive memory resident programs that may have been planted on the computer.

Your initial and primary job is to preserve the computer evidence and to transport the computer to a safe location where a complete bit stream backup of all stored data areas can be made. You also want to insure that the computer system can be reconfigured to match the configuration in which it was found.

For this purpose, it is wise to take pictures of the complete computer system from all angles. Wires should be marked such that they can be easily reconnected.

Also, the computer should be clearly marked as evidence and stored out of reach of inquiring co-workers. Chain of custody is as relevant when it comes to computers as any other form of evidence.

Law enforcement agencies have come under scrutiny in recent times regarding evidence issues. For this reason, it is important to do things right.

Be sure to properly document the time, date and circumstances surrounding the actual seizure of the computer. This helps rebut the contention later on that the evidence on the computer was planted by the computer specialist.

Every effort must be made to show that no one could have made changes to the information contained on a seized computer system. Without such an assurances, countless hours of processing effort may prove to be wasted time and the case may be lost at trial.

If seizure of the computer is carried out when the system is attended, any individual attending the computer should be immediately removed from the vicinity.

One press of a pre-arranged key combination can potentially destroy all evidence stored on a hard disk. A destructive process can be initiated in a heartbeat and the results can be disastrous. Consider using a subterfuge to remove the operator from the computer to eliminate the possibility of them destroying potential evidence.

Raid planning is very important and this is especially true if the probability of destructive processes exist.

Watch out for 'burn boxes' at the raid site which might be rigged to incinerate floppy diskettes and zip disks. I can't go into great detail in this article about their construction but they are easily constructed.

Also, avoid storing the computer components near the police car radio. The magnetic field created by the operating radio may be strong enough to destroy evidence.

A word to the wise - don't transport the seized computer in the trunk on top of the radio transmitter.

The 2nd step - purchase essential tools and equipment

Forensic computer science deals with the preservation and processing of computer evidence. Forensics is basically the application of science to the evidentiary process.

In the case of computer evidence, the science is computer science and the evidence is data stored in any number of forms on a variety of computer storage media.

Some have likened computer forensics to the autopsy of a computer. Precision and accuracy are essential in the processing of computer evidence and this can not be achieved without using the

right set of tools.

To do otherwise, would be like trying to do brain surgery with a pocketknife. Law enforcement agencies are woefully under funded. This is especially true regarding computer evidence and related technology issues.

It is tough enough for law enforcement management to pay salaries and keep a fleet of vehicles running in these tight budgetary times.

However, computer evidence is here to stay and essentially every law enforcement agency will have to deal with computer evidence issues in time.

The good news is that the price of computer technology is at an all time low. An adequate set-up that meets the minimum requirements for most small law enforcement departments can be purchased for under $6,000. This includes both computer hardware and software.

I have stressed the need for the preservation of computer evidence and the safe transport of the seized computer to a secure location so a bit stream backup can be made of all computer media.

This is required before processing of the evidence to avoid triggering potential destructive processes that may have been planted in the computer by the 'crooks'.

It also avoids the accidental overwrite of data stored in the form of erased files, in the Windows swap file, and in file slack. To process computer evidence without making bit stream backup of the 'best evidence' is like playing with fire.

You are going to get burned badly at some point. The catch is you must have the proper tools before evidence can be backed up and processed.

The price of computer hard disk drives has dropped substantially over the past year. As a result, forensic computer specialists are encountering large volumes of potential data stored on huge hard disk drives.

To put this in perspective, ten years ago a 20-megabyte hard disk drive was considered standard. Today, it is not uncommon for a desktop computer to have multiple hard disk drives with storage capacities exceeding two gigabytes per drive.

For those of you who are unfamiliar with these terms, a 20-megabyte hard disk drive has the capacity to store approximately 20 million characters of data. A two-gigabyte hard disk drive has the capacity to store approximately 100 times that capacity.

To make matters worse from a computer evidence standpoint, 5-gigabyte hard disk drives are now available and will surely find their way into police evidence lockers.

These small storage devices are not much bigger than a deck of cards but they have the potential of storing the content of hundreds of thousands of printed pages.

For these reasons, plan on spending some money on computer hard disk drives and storage media.

Even after making a bit stream backup, processing should rarely be done on the seized computer. To do so could subject the seized computer to excessive wear and tear.

Your worst nightmare might involve your expert testimony in court about how you came to break the subject computer. To avoid living this nightmare, always plan on restoring bit stream backup, made from the seized computer, to a law enforcement computer.

A lightning fast computer is normally not required. With the exception of some specialised automated fuzzy logic forensic tools, most forensic software tools operate quite nicely on lower end

Pentium based computers or the equivalent, e.g. Pentium 133 MHz to 200 MHz.

However, plenty of storage capacity is a requirement and it is also a good idea to buy at least 64 MB of Random Access Memory to insure that you will be able to run and evaluate the software retrieved from the seized computer.

Flexibility is the name of the game when you create a computer system that will be used to process computer evidence. You must be prepared to deal with the seizure a variety of computer systems and equipment configurations.

As a result, it is wise to equip your processing computer with multiple floppy disk drives, a colour SVGA monitor and plenty of external storage capacity to supplement the onboard hard disk drives.

Opinions may vary, but I recommend the following hardware configuration as a minimum system for use in computer evidence processing:

Pentium 133 MHz (or faster) tower desktop computer

SVGA 14-inch colour monitor

Two 5-GB hard disk drives

One Iomega Zip disk drive

One SyQuest SyJet (or Iomega Jazz) disk Drive

One 5.25 inch 1.2 MB floppy disk drive

One 3.5 inch 1.44 MB floppy disk drive

One CDROM (8x recommended)

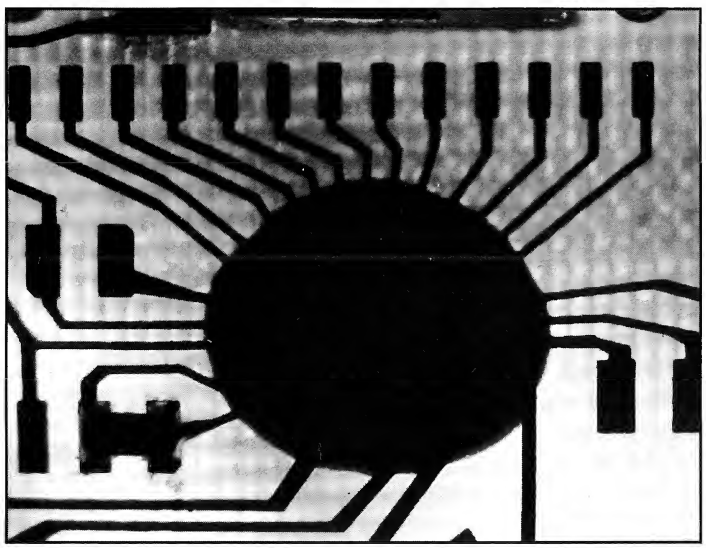
One uninterrupted power supply (UPS)

One laser printer (six pages per minute recommended)

The recommended system should meet the computer evidence needs of most small to medium sized law enforcement agencies.

As stated, this is the minimum system configuration and it should be supplemented with an adequate supply of floppy diskettes and storage cartridges, e.g. zip disks.

Further, I strongly recommend the use of a second law enforcement note-



book computer for documentation purposes. When the processing computer is used to document findings, there is a potential for parts of the text in the reports to 'cross pollinate' the backup copies of the evidence.

The potential of a memory dump into file slack is the culprit. By using a separate computer to document findings, this potential problem is eliminated.

Inexpensive notebook computers, can be purchased for under $1,000 and may come in handy for other tasks in the department as well.

Computer evidence processing can't begin without forensic software tools.

The recommended tool kit should include the following:

MS DOS 6.22 (DOS 7.0 which comes with Windows 95 is not recommended.)

Disk Management Software to take full advantage of large hard disks under DOS

Norton Disk Edit

A bit stream backup utility

A virus scanning utility

A DOS Shell utility with file view capabilities

Password recovery utilities
A text search utility

Other specialised disk utilities

Please be aware that the capacities of hard disk drives increase continually.

Normally forensic processing is performed under DOS rather than Windows, to avoid overwriting potential evidence in the form of erased files.

However, DOS will not access huge hard disk drives without disk management software.

The purchase of computer components and forensic software is a step in the right direction for most law enforcement agencies that desire to begin dealing with computer evidence issues.

The Third Step - Preserve the Electronic Crime Scene

Computer evidence is odd, to say the least. It lurks on computer hard disk drives, zip disks and floppy diskettes at three different levels - two of these levels are not visible to the computer user.

Such evidence is fragile and it can easily be destroyed through something as simple as the normal operation of the computer. Electromagnets and planted destructive Trojan horse programs are other hazards that can permanently destroy computer evidence in seconds.

I cannot think of any other type of evidence that presents the investigator with as many potential problems and challenges. In the old days defence lawyers didn't know much about computer evidence. As a result, cross-examination by the defence went pretty easy a few years ago.

However, things are changing because lawyers are becoming educated due to the current popularity of electronic document discovery in the legal community.

Times have changed and it is all the more important to do things by the book.

The computer investigator not only needs to be worried about destructive process and devices being planted by the computer owner. He or she also needs to be concerned about the operating system of the computer and applications.

Evidence is easily found in typical storage areas, e.g., spreadsheet, database and word processing files. Unfortunately potential evidence can also reside in file slack, erased files and the Windows swap file.

Such evidence is usually in the form of data fragments and it can be easily overwritten by something as simple as the booting of the computer and/or the running Microsoft Windows.

When Windows starts, it potentially creates new files and opens existing ones as a normal process. This situation can cause erased files to be overwritten and data previously stored in the Windows swap file can be altered or destroyed.

Furthermore, Windows 95 has a habit of updating directory entries for files as a normal operating process. As you can imagine, file dates are very important from an evidence standpoint.

Another concern of the computer investigator, is the running of any programs on the subject computer. Criminals can easily modify the operating system to destroy evidence when standard operating systems commands are executed.

In the training courses that I teach, I have the students modify the operating system such that the execution of the DIR command destroys simulated evidence.

Standard program names and familiar Windows program icons can also be altered and tied to destructive processes by a crafty high tech criminal.

Even trusted word processing programs like Microsoft Word and WordPerfect can become the enemy of the cyber cop. It works this way - when word processing files are opened and viewed, temporary files are created by the word processing program.

These files overwrite the temporary files that existed previously and potential evidence stored in those files can be lost forever. I hope I am starting to make my point.

Computer evidence processing is risky business and is fraught with potential problems. Of course, any loss of crucial evidence or material falls on the shoulders of the computer investigator.

What will your answer be, if the defence attorney claims the data you destroyed proved the innocence of his client? You better have a good answer.

Many inherent problems associated with computer evidence processing vanish when tried and proven processing procedures are followed. When it comes to computer evidence processing, Murphy is always looking over your shoulder. He stands ready to strike at just the wrong moment.

Your very first objective, after securing the computer, should be to make a complete bit stream backup of all computer data before it is reviewed or processed. This should normally be done before the computer is operated.

Preservation of evidence is the primary element of all criminal investigations and computer evidence is certainly no exception. This basic rule of evidence never changes.

Even rookies know that evidence must be preserved at all costs.

As stated previously, evidence can reside at multiple levels and in bizarre storage locations.

These levels include allocated files, file slack and erased files. It is not enough to do a standard backup of a hard disk drive. To do so would eliminate the back up of file slack and erased file space. Without backing up evidence in these unique areas, the evidence is susceptible to damage and/or modification by the computer investigator.

Bit stream backups are much more thorough than standard backups. They involve the copying of every bit of data on a storage device and I usually recommend that two such copies be made of the original when hard disk drives are involved.

Any processing should be performed on one of the backup copies. As I stressed before, the original evidence should be preserved at all costs. After all, it is the 'best evidence'.

The need for forensic bit stream image backups was identified by a group of us back in late 1989 during the creation of the first computer forensic science training courses at the Federal Law Enforcement Training Center.

The very first program created to perform this task was named IMDUMP and it was developed by Michael White, who was employed by Paul Mace Software.

That program proved to be helpful until approximately 1991 when most of the Paul Mace utilities were sold to another software company.

Lacking the continued support for IMDUMP, we went to Chuck Guzis at Sydex Corporation in Eugene, Oregon and presented him with our dilemma.

Chuck had been a friend of law enforcement computer specialists for years and our begging paid off. He agreed to develop a specialised program that would meet our bit stream backup needs from an evidence standpoint.

I like to think of Chuck as the father of electronic crime scene preservation and the resulting program, SafeBack, has become a law enforcement standard.

In addition, it is used by numerous government intelligence agencies, military agencies and law enforcement agencies world wide.

Another bit stream backup program called SnapBack is also available and is used by some law enforcement agencies primarily because of its ease of use.

It is priced several hundreds of dollars higher than SafeBack and its original design was not for evidence processing. It was designed as a network backup utility for use by system administrators.

SafeBack was designed from the ground up as an evidence-processing tool and is priced to fit law enforcement budgets.

It has error checking built into every phase of the evidence backup and restoration process.

I prefer SafeBack but it may come down to price or personal preference.

For more information about SafeBack, please check out the Sydex web site at www.sydex.com/forensic.html.

The important thing is to make a bit stream backup of all computer data before you begin processing.

I can't stress the importance of bit stream image backups enough. To process a computer hard disk drive for evidence without one is like playing with fire in a gas station.

The basic rule is that only on rare occasion should you process computer evidence without making an image backup first. The hard disk drive should be imaged using a specialised bit stream backup product and the floppy diskettes can be imaged using the standard DOS DISKCOPY program.

Directions should be followed exactly regarding the use of the bit stream backup software.

When DOS DISKCOPY is used, it is recommended that MS DOS Version 6.22 be used and the /V (data verification) switch should be invoked from the command line.

To avoid getting too technical for the purposes of this article, I will avoid going into the specifics regarding the uses of these backup programs.

However, instruction manuals should be studied thoroughly before you attempt to process computer evidence. Ideally, you should conduct tests on your own computers beforehand and compare the results with the original.

Being comfortable with the software you use is an important part of computer evidence processing. One of the original computer evidence masters, Stephen Choy, puts it nicely when he says, "Know your tools".

Practice using all of your forensic software tools before you ever use them in the processing of computer evidence. You may only get one chance to do it right..

The author, **Michael R. Anderson**, is the President and primary founder of New Technologies Inc, based in Oregon, US. Mr. Anderson's professional background includes 25 years as a Special Agent/Computer Specialist with the Criminal Investigation Division of the Internal Revenue Service.

Since 1987, Mr. Anderson has been instrumental in the development of computer evidence training courses and related forensic software tools for the Internal Revenue Service and the International Association of Computer Investigative Specialists (IACIS).

NTI specialises in the fields of forensic computer science, cryptanalysis, forensic utility software development, computer artificial intelligence and computer security risk identification.

The firm can be contacted on +1 503 666 6599 or by e-mail to info@forensics-intl.com

Computer security

Reported computer crime is just the tip of the iceberg, and action has to be taken now to stop the problem getting worse, writes Ian Hayward.

There have been many articles written in the popular press about the unauthorised use of computer systems by outsiders, a practice that has been called "hacking".

The media appears to follow the concept that virtually any crime that even involves the use of a computer fits the description of "hacking". While the actual number of "hacking" cases reported by business to various authorities has been estimated at approximately nine per cent of computer abuse incidents, recent reports in the press indicate that it is becoming a more significant problem as more computers become interconnected.

A large number of computer Bulletin Board Systems (BBS) are now connected to the Internet, this allows those members with sufficient access rights to connect to computers anywhere.

These BBS's are known to have file areas dealing with hacking activities, and covering a wide range of computer operating systems. In fact some BBS's have been known to keep files detailing methods for bypassing security measures by obtaining a copy of the password file on a system. I found a program on one of these BBS's that enables the user to generate up to 999 legitimate credit card numbers from one card number.

It seems very surprising that the reported incidence of hacking is such a low figure. Can we therefore assume that very few cases are ever reported to the authorities, or is it simply that a very small percentage of the incidents are detected and the perpetrators prosecuted?

My own opinion is that both of these apply in Australia and I feel sure that the actual cases which are reported in the media are only the tip of the iceberg.

In fact, only a very small percentage of the cases of computer abuse are ever reported to the police authorities. The majority of businesses are unlikely to report any incident to the police authorities for fear of it becoming public knowledge when and if a case goes to trial.

The effects on a business from the publication of details of a computer abuse/fraud incident may well range from a drop in share prices through to a loss of business.

If we consider crime in general, we must remember that the majority of crimes are committed by criminals who are never convicted for them. This infers that the majority of the information gathered by organisations actually relates to the cases of failed criminals, that is the ones that were caught and convicted.

Indeed it is quite apparent that the majority of hacking cases are never even detected, let alone reported to authorities. Business itself appears to maintain an attitude characterised by its own self-interest, rather then any need of the general public to know of any such hacking. Generally any incident involving computer abuse is kept "in-house" and there is little likelihood of any prosecution of the offender.

Companies have been known to give an offender a glowing reference to ensure they obtain employment with another company, thus getting rid of their own problem. If we are to have any chance of reducing the occurrence of this computer crime and its consequent cost to the community as a whole, there is an obvious need for greater co-operation and data sharing.

If this data and the experiences of all interested parties, including police authorities, researchers and businesses, were to be shared there would likely be other areas of computer security and indeed fraud in general that could not only be highlighted, but may in fact be reduced by a combined effort.

Artificial intelligence has been proposed in some areas as a means of reducing the abuse of computer systems by monitoring the actual use made by users. This monitoring gathers information of the users' past behaviour while using the computer and highlights any noticeable changes in their present usage. While this method can only detect a crime after it has been committed, it could be developed into a deterrent.

Other types of security measures have been aimed at using artificial intelligence to develop methods of controlling access to computer systems which are based on the use of an individual's physical characteristics, such as fingerprints, retina scans and hand geometry.

These methods will significantly deter outsiders attempting to access a computer system, but they will not completely prevent an insider from gaining access to information and computer resources that they should not be using.

Criminal organisations throughout the world have always been ready to employ whatever technology is available to enhance their business activities. We have only to look at the increase in the electronic exchange of monies between various countries, which has occurred whenever there is an increase in criminal activity.

The criminal elements of society have shown they are quite willing to use various means to corrupt both business and politics. Using these same methods, they could easily gain the expertise needed for them to commit both major and minor computer based crimes.

This computer technology must now pose a threat to society when it can be used by organised crime not only in their traditional crime areas, but also in the white-collar crime area.

In this way there is every possibility that the extent and spread of organised crime networks may increase dramatically. Using readily available facilities such as e-mail and talk, the criminal community can communicate throughout the world 24 hours a day without any fear of detection.

If they were to communicate via telephone or radio they run the risk of any number of law enforcement agencies using bugging devices and/or taps of one sort or another to listen in to their communications.

Obviously there is a great deal of scope for research to be undertaken in the application of artificial intelligence techniques and/or software packages to the computer crime arena. These could be used not only for educating the management of business organisations in security risks, but also as an aid to determine the security risks associated with both computer systems and their users.

Ian Hayward is a former lecturer in business computing, Victoria University of Technology, Melbourne, Victoria.

Notice Board

We will be pleased to receive contributions to this page. Please mark all correspondence 'Notice Board'. We reserve the right to edit if required.

Events

IACON '98 The Internal Audit Conference

24-25 February 1998, London, UK

Now in its seventh year, the conference offers six themes which will cover: Risk Management; Audit Automation; CRSA; Innovative Approaches to Audit; Re-Engineering Audit and Fraud.

IACON also features two interactive workshops: CRSA: What Approach Is Right For You and Leading Edge IT Risk Management Strategies For SAP R/3 And Corporate Networks.

Contact: IIR Ltd
Tel: 0171 915 5182
Fax: 0171 393 0313

Securing Data Transmissions - An Encryption Primer

24 February 1998
Bristol, UK

Intensive workshop course includes: How Codes And Ciphers Work - how they are used to protect sensitive data, how digital signatures are used to authenticate transmissions, how to decide an appropriate cryptographic strategy.

Contact: System Security Training Centre

Tel: 01625 523205
Fax: 01625 526952

Money Laundering in Central and Eastern Europe

5-6 March 1998
Kempinksi Hotel Corvinus,
Budapest, Hungary

The second annual conference on money laundering in Central and Eastern Europe offers a practical guide to the problems and progress towards solutions. An international panel of speakers will provide insights into such topics as organised crime, international co-operation in law enforcement and harmonisation with the European Union. One section of the programme will provide a practical examination of the particular problems affecting different sectors of the financial marketplace - the banking sector, securities trading and electronic money/the Internet - and the measures which can be taken to combat these problems. Case studies will also be presented.

Contact: Int. Conference Group

Tel: +44(0)181 743 8787
Fax: +44(0)181 740 1717

Forensic Computing Conference '98

24-25 March 1998
University of Warwick Conference Park,
Coventry, UK

The conference is hosted by a multi-agency (UK) group, known as the Forensic Computing Group. The objectives of the group are "to foster better awareness and appreciation of the potential for evidence from computers, to provide good practice in the recovery of such evidence and to act as a national focus for dissemination of information concerning developments in this field."

The theme of the conference will be 'Common Computer Forensic Standards'.

Contact: Conference Secretariat
Tel: +44(0)1442 828200
Fax: +44(0)1441 828288

Workshop on Information Hiding

15-17 April 1998, Portland, Oregon, US

Call for papers

Many researchers are interested in projects about information hiding. Research themes include copyright marketing of digital objects, covert channels in computer systems, subliminal channels in crytpographic protocols, low probability of intercept communications, broadcast encryption schemes and various kinds of anonymity services ranging from steganography to location security.

The second international workshop on information hiding will take place in Oregon and those interested in submitting papers should contact the program chair, David Aucsmith, by e-mail on awk@ibeam.intel.com

Internet World UK

May 12 - 14, Olympia 2, London, UK
Contact: +44 (0)1865 388000

Annual Conference for Data Protection Officers

May 13, Manchester, UK
Price - £149, organised by Keep IT Legal
Contact +44 (0)1246 473999

Securing and Auditing Internet Connections

21 May 1998
Bristol, UK

The security module of this course includes: Where the Main Risks Lie; Hackers and Spoofers; Virus and Trojan Horse Attacks; Locating Audit Resources on the Internet; Privacy and Data Security - legal issues, building a firewall, secure gateways, encryption techniques (DES and PGP), digital signatures and user authentication techniques.

Contact: Int. Conference Group
Tel: +44(0)181 743 8787
Fax: +44(0)181 740 1717

International Journal of FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd.